UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,521	06/06/2000	Upendra V. Chaudhari	YOR9-2000-0093US1(8728-35	8243

7590 12/30/2003

Frank Chau Esq
F Chau & Associates LLP
Suite 501
1900 Hempstead Turnpike
East Meadow, NY 11554

EXAMINER	
QUINONES, EDEL H	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/30/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/588,521	CHAUDHARI ET AL.	
	Examiner	Art Unit	
	Edel H Quinones	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *06 June 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

III. Detailed Action

1. Claims 1-28 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1 and 12 are rejected under 35 U.S.C. 102(b) as being anticipated by Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter).

In regards to claims 1 and 12, Kanevsky teaches a system for authenticating a user in a conversational system (col. 1, lines 15-19), comprising the steps of: receiving an identity claim from a user (i.e. receiving first spoken utterances of the speaker, the first spoken utterances containing indicia of the speaker) (col. 3, lines 23-25); computing a confidence score based on the identity claim using speech input from the user, wherein the confidence score is a measure of confidence in the validity of the identity claim (col. 3, lines 41-43); providing the user access to secured data based on the computed confidence score (col. 3, lines 44-48).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2, 7, 13 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of Diep (U.S. Patent 6,370,648).

Kanevsky teaches claims 1 and 12 as discussed above.

In regards to claim 2 and 13, Kanevsky, does not teach further comprising the step of maintaining the confidence score as part of the system state.

Diep teaches further comprising the step of maintaining the confidence score as part of the system state (i.e. the closeness factor or score from the match is stored in memory by the security program at step 508) (col. 8, lines 5-6).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Diep to include further comprising the step of maintaining the confidence score as part of the system state with the motivation to provide a definition of closeness between two command sequences that is easy to interpret and manipulate by a network intrusion program (Diep, col. 2, lines 64-67).

In regards to claims 7 and 18, Kanevsky does not teach further comprising the step of re-computing the confidence score upon an occurrence of a predetermined event.

Diep teaches further comprising the step of re-computing the confidence score upon an occurrence of a predetermined event (i.e. the matching process of FIG. 5 can be done multiple times for the same user or for multiple users throughout a predetermined time period, such as a day) (col. 8, lines 15-17).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Diep to include further comprising the step of re-computing the confidence score upon an occurrence of a predetermined event with the motivation to provide a definition of closeness between two command sequences that is easy to interpret and manipulate by a network intrusion program (Diep, col. 2, lines 64-67).

5. Claims 3-16, and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of Fritch el al. (U.S. Patent 6,105,132 and Fritch hereinafter).

Kanevsky teaches claims 1 and 12 as discussed above.

In regards to claims 3 and 14, Kanevsky does not teach further comprising the steps of partitioning the secured data into a plurality of data classes; assigning a security level to each of the data classes; and constructing an access map based on the security levels for accessing the secured data.

Fritch teaches further comprising the steps of partitioning the secured data into a plurality of data classes (i.e. classification levels) (col. 1, line 50); assigning a security level to each of the data classes (col. 6, lines 34-37); and constructing an access map based on the security levels for accessing the secured data (col. 8, lines 28-30).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Fritch to include further comprising the steps of partitioning the secured data into a plurality of data classes;

assigning a security level to each of the data classes; and constructing an access map based on the security levels for accessing the secured data with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

In regards to claims 4 and 15, Kanevsky does not teach further comprising the steps of selecting a range of confidence scores; partitioning the range of confidence scores into a plurality of regions; and assigning each region to one of the security levels.

Fritch teaches further comprising the steps of selecting a range of confidence scores (i.e. users and/or tasks) (col. 2, lines 64); partitioning the range of confidence scores into a plurality of regions (i.e. clearance levels) (col. 6, line 18-20); and assigning each region to one of the security levels (i.e. determining the access rights of the task and/or user with respect to a particular information object or class of information objects) (col. 8, lines 28-30).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Fritch to include further comprising the steps of selecting a range of confidence scores; partitioning the range of confidence scores into a plurality of regions; and assigning each region to one of the security levels with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

In regards to claims 5 and 16, Kanevsky does not teach wherein the step of providing the user access to secured data based on the computed confidence score comprises the steps of: determining a given region of the plurality of regions which comprises the computed confidence score; determining the security level assigned to the given region; and accessing secured data using the access map based on the security level assigned to the given region.

Fritch teaches wherein the step of providing the user access to secured data based on the computed confidence score comprises the steps of: determining a given region (i.e. clearance levels) (col. 6, line 18-20) of the plurality of regions which comprises the computed confidence score (i.e. users and/or tasks) (col. 2, lines 64); determining the security level (i.e. classification levels) (col. 1, line 50) assigned to the given region; and accessing secured data using the access map based on the security level assigned to the given region (col. 8, lines 28-67).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Fritch to include wherein the step of providing the user access to secured data based on the computed confidence score comprises the steps of: determining a given region of the plurality of regions which comprises the computed confidence score; determining the security level assigned to the given region; and accessing secured data using the access map based on the security level assigned to the given region with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

In regards to claims 6 and 17, Kanevsky does not teach wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned to at least one security level that is lower than the security level of the given region.

Fritch teaches wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned to at least one security level that is lower than the security level of the given region (i.e. one suitable policy implements the familiar Bell-LaPadula model, which

may be summarized by the rule "No read up" and "No write down." That is the task cannot read from information objects that are more sensitive, and cannot write to objects that are less sensitive, that the sensitivity level [effective clearance level(s)] of the task itself.) (col. 8, lines 40-45).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of Fritch to include wherein the step of accessing secured data using the access map comprises the step of allowing access to secured data that is assigned to the security level of the given region and secured data assigned to at least one security level that is lower than the security level of the given region with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

6. Claims 8 and 19 rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of Diep (U.S. Patent 6,370,648) as applied to claims 7 and 18 above, in further view of French et al. (U.S. Patent 6,321,339 and French hereinafter).

The combination of Kanevsky and Diep teaches claims 7 and 18 as discussed above.

The combination of Kanevsky and Diep does not teach wherein the predetermined event is a user query for accessing secured data.

French teaches wherein the predetermined event is a user query for accessing secured data (i.e. matching routines, implemented for each data source and type of check, compare query data to known source data and preferably assign a value to every match instance. This value may be termed an authenticity certainty score) (col. 12, lines 8-12).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Kanevsky and Diep with the teachings of French to include wherein the predetermined event is a user query for accessing secured data with the motivation of enabling different levels of authentication to be performed based on the level of security desired, thus reducing costs and unnecessary use of system resources (French, col. 2, lines 62-65).

7. Claims 9-11 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of French et al. (U.S. Patent 6,321,339 and French hereinafter).

Kanevsky teaches claims 1 and 12 as discussed above.

In regards to claims 9 and 20, Kanevsky does not teach wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions.

French teaches wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions (i.e. additionally, the checks of preprocessing step 26 may include the use of a credit card application fraud model, or some other model which statistically analyzes response data. For example, the data supplied by the user may be modeled and graded for confidence level based upon empirical models supplied by third party vendors or available internally) (col. 11, lines 42-47).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky with the teachings of French to

include wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions with the motivation of enabling different levels of authentication to be performed based on the level of security desired, thus reducing costs and unnecessary use of system resources (French, col. 2, lines 62-65).

In regards to claims 10 and 21, Kanevsky teaches wherein the confidence score comprises one of (1) a first component for considering a single mode implementation and (2) the first component and a second component for considering a multi-modal implementation (i.e. it is further to be understood that P(acoustic data|speaker$_i$) may be computed using some acoustic models for speakers that may be represented as Hidden Markov Models (HMM)) (col. 11, lines 15-17). The Examiner interprets a Hidden Markov Model representation as a single mode implementation.

In regards to claims 11 and 22, Kanevsky teaches wherein the confidence score comprises a mixing factor for weighting the first and second component in a multi-modal implementation (i.e. in another embodiment, one can interpret P(speaker$_i$) as a weighted factor and update a general speaker score using a known formula) (col. 11, lines 18-20). The Examiner interprets the P(speaker$_i$) value to be equivalent to the confidence score.

8. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of Diep (U.S. Patent 6,370,648) as applied to claim 18 above, in further view of Fritch el al. (U.S. Patent 6,105,132 and Fritch hereinafter).

In regards to claim 23, the combination of Kanevsky and Diep, as applied to claim 18 above, teaches a computation module for periodically computing a confidence score during a dialog session with at least one user seeking access to data in the database, wherein the confidence score is a measure of confidence in the validity of an original identity claim provided at a commencement of the dialog session.

The combination does not teach a database that is partitioned into a plurality of data classes, wherein each data class is assigned a range of confidence scores based on a security level of the data class; and a dialog manager for controlling access to data in the database based on a last computed confidence score.

Fritch teaches a database (i.e. a program, functions, and/or instructions) (col. 5, line 6) that is partitioned into a plurality of data classes, wherein each data class is assigned a range of confidence scores based on a security level of the data class (col. 6, lines 34-46); and a dialog manager for controlling access to data in the database based on a last computed confidence score.

Fritch teaches that one of the many computer networks suited for use with the present invention is indicated generally at 10 in FIG. 1. In one embodiment, the network 10 includes Novell NetWare.RTM. network operating system software (NETWARE is a registered trademark of Novell, Inc.). In alternative embodiments, the network includes NetWare Connect Services, VINES, Windows NT, Windows 95, LAN Manager, or LANtastic network operating system software and/or an implementation of a distributed hierarchical partitioned object database according to the X.500 protocol (VINES is a trademark of Banyan Systems; NT, WINDOWS 95, and LAN MANAGER are trademarks of Microsoft Corporation; LANTASTIC is a trademark of Artisoft). The network 10 may include a local area network 12 which is

connectable to other networks 14, including other LANs or portions of the Internet or an intranet, through a gateway or similar mechanism. (col. 4, lines 16-32). The Office interprets the above as a database and a dialog manager.

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Kanevsky and Diep with the teachings of Fritch to include a database that is partitioned into a plurality of data classes, wherein each data class is assigned a range of confidence scores based on a security level of the data class; and a dialog manager for controlling access to data in the database based on a last computed confidence score with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

In regards to claim 24, the combination of Kanevsky and Diep does not teach further comprising an access map for mapping each data class with the corresponding range of confidence scores, wherein the access map is utilized by the dialog manager to provide access to data based on the last computed confidence score.

Fritch teaches further comprising an access map for mapping each data class with the corresponding range of confidence scores, wherein the access map is utilized by the dialog manager to provide access to data based on the last computed confidence score (col. 8, lines 28-30).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Kanevsky and Diep with the teachings of Fritch to include further comprising an access map for mapping each data class with the corresponding range of confidence scores, wherein the access map is utilized by the dialog

manager to provide access to data based on the last computed confidence score with the motivation to provide a consistent access policy in a computer network (Fritch, col. 2, lines 28-29).

In regards to claim 25, Diep teaches further comprising means for maintaining the last computed confidence score as part of the system state (i.e. the closeness factor or score from the match is stored in memory by the security program at step 508) (col. 8, lines 5-6).

9. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanevsky et al. (U.S. Patent 5,897,616 and Kanevsky hereinafter) in view of Diep (U.S. Patent 6,370,648) in further view of Fritch el al. (U.S. Patent 6,105,132 and Fritch hereinafter) as applied to claim 23 above, and further in view of French et al. (U.S. Patent 6,321,339 and French hereinafter).

The combination of Kanevsky, Diep, and Fritch disclose claim 23 as discussed above.

In regards to claim 26, the combination of Kanevsky, Diep, and Fritch does not teach wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions.

French teaches wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions (i.e. Additionally, the checks of preprocessing step 26 may include the use of a credit card application fraud model, or some other model which statistically analyzes response data. For example, the data supplied by the user may be modeled and graded for confidence level based upon empirical models supplied by third party vendors or available internally) (col. 11, lines 42-47).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Kanevsky, Diep, and Fritch with the teachings of French to include wherein the confidence score is based on a linear function of statistical models that characterize the score under a plurality of conditions with the motivation of enabling different levels of authentication to be performed based on the level of security desired, thus reducing costs and unnecessary use of system resources (French, col. 2, lines 62-65).

In regards to claim 27, Kanevsky teaches wherein the confidence score comprises one of (1) a first component for considering a single mode implementation and (2) the first component and a second component for considering a multi-modal implementation (i.e. it is further to be understood that P(acoustic data|speaker$_i$) may be computed using some acoustic models for speakers that may be represented as Hidden Markov Models (HMM)) (col. 11, lines 15-17). The Examiner interprets a Hidden Markov Model representation as a single mode implementation.

In regards to claim 28, Kanevsky teaches wherein the confidence score comprises a mixing factor for weighting the first and second component in a multi-modal implementation (i.e. in another embodiment, one can interpret P(speaker$_i$) as a weighted factor and update a general speaker score using a known formula) (col. 11, lines 18-20). The Examiner interprets the P(speaker$_i$) value to be equivalent to the confidence score.

Other Prior Art Made of Record

10. A. Trandal et al. (US Patent No. 6,088,428) discloses a voice controlled messaging system and processing method; and

B. Gressel (US Patent No. 6,311,272) discloses a biometric system and techniques suitable therefor.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H Quiñones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheik can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quinones
Patent Examiner
Technology Center 2100

December 23, 2003

EMMANUEL L. MOISE
PRIMARY EXAMINER